Delusions of Adequacy? Examining the Case for Finding the United States Adequate for Cross-Border EU-U.S. Data Transfers

Christopher Wolf*

This Article explores the European Union (EU) adequacy mechanism for assessing cross-border data flows, and highlights where U.S. law aligns with and differs from the EU approach to privacy. Following the Introduction, Part I explains how the EU adequacy mechanism works and how it has been applied in practice. Parts II and III then review the case for and against U.S. privacy law being deemed adequate under the EU privacy framework. The Article concludes with some thoughts on how cross-border data flows can be managed as both the United States and EU contemplate new privacy laws and a new transatlantic trade agreement.

INTRODUCTION

Following the revelations by Edward Snowden about the nature and extent of NSA surveillance in the summer of 2013, officials in the EU mounted an aggressive war of words directed at the United States and questioned the commitment of its government and corporations to personal privacy.[1] The openly hostile challenge to U.S. privacy marked a dramatic change in tone and substance in the EU's approach to cross-border cooperation on privacy. A little over a

* Christopher Wolf is a director of the global Privacy and Information Management practice at Hogan Lovells US LLP, and is the founder and co-chair of the Future of Privacy Forum think tank. In the spring of 2013, following the announcement of EU-U.S. negotiations towards a Transatlantic Trade and Investment Partnership (TTIP), he was a lead organizer of the Coalition for Privacy and Free Trade. Special thanks to Hogan Lovells colleagues Paul Otto and Julian Flamant for their substantial assistance in the preparation of this Article.

1. *See* Christopher Wolf, *The Brussels and Warsaw Privacy Peace Talks*, PRIVACY PERSPECTIVES (Aug. 29, 2013), https://www.privacyassociation.org/privacy_perspectives/post/the_brussels_and_warsaw_privacy_peace_talks.

year before, there appeared to be a thaw in the transatlantic privacy relationship:

> The United States and the European Union clearly share a commitment to promoting the rights of individuals to have their personal data protected and to facilitating interoperability of our commercial data privacy regimes.
>
> The European Union and the United States are global leaders in protecting individual freedoms, including privacy, while at the same time fostering innovation and trade that are so critical to the world economy, notably in the present times. Stronger transatlantic cooperation in the field of data protection will enhance consumer trust and promote the continued growth of the global Internet economy and the evolving digital transatlantic common market.[2]

In March 2012, the European Commission Directorate-General for Justice, Fundamental Rights, and Citizenship ("DG Justice") hosted a conference on "Privacy and Protection of Personal Data" that was held simultaneously in Washington, D.C., (at the U.S. Institute of Peace) and in Brussels, in which senior officials of the Commission, the Obama administration, the Federal Trade Commission (FTC), NGOs, and corporate representatives participated. As reflected in the agenda[3] and in the Joint Statement of European Commission Vice President Reding and then-U.S. Commerce Secretary Bryson, the gathering was intended to explore the "common principles" of the two jurisdictions, heralded as "partners," with a focus on "compatibility, compliance and accountability at global scale."[4] The borderless nature of the Internet and the global nature of digital trade

2. Press Release, Joint European Statement on Data Protection by European Commission Vice-President Viviane Reding and U.S. Secretary of Commerce John Bryson (Mar. 19, 2012), *available at* http://europa.eu/rapid/press-release_MEMO-12-192_en.htm [hereinafter EU-U.S. Joint Statement].

3. Press Release, European Commission, EU Conference: Privacy and Protection of Personal Data (Mar. 19, 2012), *available at* http://ec.europa.eu/justice/data-protection/files/eu-us-data-programme_en.pdf; *see also id.*

4. EU-U.S. Joint Statement, *supra* note 2.

was recognized as a strong motivation to identify common and compatible approaches to the protection of personal data.[5]

Yet, the jointly acknowledged "shared commitment" and "joint leadership," and the need for "stronger transatlantic cooperation" on privacy, have not changed the innate opinion of the relevant European authorities—exacerbated by the Snowden episode—that the U.S. privacy framework is "inadequate," an opinion that hinders or encumbers cross-border data flows and, ultimately, international trade and economic growth.[6] In truth, the United States has never formally requested an adequacy determination (beyond that for the limited EU-U.S. Safe Harbor framework[7]), likely because of the well-understood outcome: request denied.

Just over a year after the European Commission's March 2012 "charm offensive" at the Institute of Peace session, in which a thaw in EU-U.S. privacy relations seemed possible, FTC Commissioner Julie Brill went to Brussels to reprise the favorable comparison of the EU and U.S. privacy regimes.[8] The speech she gave came at a time when the proposed EU Regulation was entering crucial consideration in the European Parliament and when European perceptions of significant (negative) differences between the EU and U.S. regimes were intensifying.[9] Commissioner Brill reminded Europeans there is a "central reality that lies at the interface between EU and U.S. privacy law: while many commenters dwell on the significant differences between the EU and U.S. privacy regimes, I believe it is important to recognize that we also have much in common."[10] Indeed, both the U.S. and EU privacy frameworks are based on the "Fair Information Practice Principles" (FIPPs), "first articulated in a comprehensive manner in the United States Department of Health,

5. *EU-U.S. Joint Commitments On Privacy And Protection Of Personal Data*, EDRI-GRAM (Mar. 28, 2012), http://www.edri.org/edrigram/number10.6/eu-us-privacy-commitments.

6. U.S. INT'L TRADE COMM'N, DIGITAL TRADE IN THE U.S. & GLOBAL ECONS., PART 1 5–12 (Jul. 2013), *available at* http://www.usitc.gov/publications/332/pub4415.pdf.

7. *See infra* note 128.

8. Frances Robinson, *U.S. to EU: U.S. Data Law is Brill*, WALL ST. J. BLOGS (Apr. 19, 2013, 11:45 AM), http://blogs.wsj.com/brussels/2013/04/19/u-s-to-eu-u-s-data-law-is-brill/.

9. *FTC's Brill Addresses EU on Privacy*, INTERNET ASS'N (Apr. 23, 2013), http://internetassociation.tumblr.com/post/48689421851/ftcs-brill-addresses-eu-on-privacy.

10. Julie Brill, Remarks to the Mentor Group for EU-U.S. Legal-Economic Affairs 1 (Apr. 16, 2013), *available at* http://www.ftc.gov/speeches/brill/130416mentorgroup.pdf.

Education, and Welfare's seminal 1973 report entitled *Records, Computers and the Rights of Citizens*, and following which "a canon of fair information practice principles has been developed by a variety of governmental and inter-governmental agencies,"[11] such as the privacy guidelines issued in 1980 by the Organization for Economic Co-operation and Development (OECD).[12] The EU and United States have taken divergent approaches to implementing the FIPPs.[13] In the United States, where privacy interests are balanced with the right to free expression, and in recognition of the fact that—as a practical matter—not every piece of personal information can be protected and policed, the framework provides the highest levels of protection for sensitive personal information—such as health,[14] financial,[15] and children's[16] information. In addition, targeted enforcement actions against bad (or negligent) actors—principally by the FTC—have created a "common law" of what is expected from business when it comes to the collection, use, and protection of personal information.[17] A web of state data security and data security breach notification laws, as well as enforcement actions at the state level in the United States, have added to the protections for personal data consistent with the FIPPs.[18]

---

11. FTC, PRIVACY ONLINE: A REPORT TO CONGRESS 48 n.27 (Jun. 1998), *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf.

12. OECD, GUIDELINES ON THE PROT. OF PRIVACY & TRANSBORDER FLOWS OF PERSONAL DATA (1980), *available at* http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

13. Christopher Wolf & Winston Maxwell, *So Close, Yet So Far Apart: the EU and U.S. Visions of a New Privacy Framework*, ANTITRUST 8 (summer 2012), *available at* http://law.duke.edu/sites/default/files/images/centers/judicialstudies/Visions_New_Privacy_ Framework.pdf.

14. *See, e.g.*, the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29 and 42 U.S.C.), and its implementing regulations.

15. *See, e.g.*, the Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified in scattered sections of 12 and 15 U.S.C.), and its implementing regulations.

16. *See, e.g.*, the Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–07, and its implementing regulations.

17. Daniel Solove & Woodrow Hartzog, *The FTC and The New Common Law of Privacy*, 114 COLUM. L. REV. 23 (forthcoming 2014), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312913.

18. *See* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 292 (2011).

The U.S. privacy framework is far from perfect. New technologies for the collection, combination, and sharing of personal data allow some privacy-insensitive businesses to act inconsistently with consumer expectations, or to act with little to no transparency, and even well-intentioned businesses sometimes push the envelope in terms of data collection and use.

The EU privacy law regime purports to deal with the U.S. imperfections by providing substantive protections for all personal data. In reality, however, the broad protections are not matched by EU enforcement of those protections. The European Union's 1995 Data Protection Directive[19] (the "Directive") lays out prescriptive rules regarding the processing—including collection, storage, use, and disclosure—of all personal data.[20] The EU enacted the Directive following the creation of the EU, in large part to harmonize its Member States' laws to facilitate the transfer of personal data among Member States while ensuring similar levels of data protection.[21] The level of EU protection is in furtherance of Article 8 of the Charter of Fundamental Rights of the European Union, which provides:

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.

---

19. *See* Council Directive 95/46, 1995 O.J. (L 281) 31, *available at* http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf [hereinafter Council Directive 95/46].

20. *See* Council Directive 95/46, *supra* note 19, art. 3(1) ("This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.").

21. *See* Council Directive 95/46, *supra* note 19, Recital 8 ("Whereas, in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States; whereas this objective is vital to the internal market but cannot be achieved by the Member States alone, especially in view of the scale of the divergences which currently exist between the relevant laws in the Member States and the need to coordinate the laws of the Member States so as to ensure that the cross-border flow of personal data is regulated in a consistent manner that is in keeping with the objective of the internal market as provided for in Article 7a of the Treaty; whereas Community action to approximate those laws is therefore needed.").

3. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

4. Compliance with these rules shall be subject to control by an independent authority.[22]

A major difference between the U.S. and EU privacy regimes is the way in which each regulates cross-border data flows. In the United States, enforcement of privacy protections across borders has "relied on holding those who transfer data accountable for its safe-keeping, and self-regulatory codes of conduct to protect the privacy of personal information that flows across borders."[23] The EU, on the other hand, has a more formal approach. Article 25 of the Directive generally prohibits transfers of personal data to a third country unless that third country "ensures an adequate level of protection."[24]

The United States' approach to cross-border transfers is consistent with the OECD's 1980 privacy guidelines that do not require evaluating the "adequacy" of third countries' privacy practices for purposes of data transfer, and that specifically address the need for countries to facilitate cross-border data transfers.[25] The Asia-Pacific Economic Cooperation (APEC) Privacy Framework, issued in 2005, covers a wide range of privacy protections but does not involve the process of making adequacy determinations. The APEC Privacy Framework instead opts for an accountability principle: "When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or

22. Charter of Fundamental Rights of the European Union, 2000 O.J. (C 364) 1, *available at* http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

23. Brill, *supra* note 10, at 5.

24. Council Directive 95/46, *supra* note 19, art. 25(1) ("The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.").

25. OECD, *supra* note 12, para. 20 ("Member countries should also ensure that procedures for transborder flows of personal data and for the protection of privacy and individual liberties are *simple and compatible with* those of other Member countries which comply with these Guidelines." (emphasis added)); *see also id.* para. 20, explanatory memorandum paras. 71–73 (discussing the need for international cooperation).

exercise due diligence and take reasonable steps to ensure the recipient person or organization will protect the information consistently with these Principles."[26]

That is not to say that the adequacy approach exists solely in Europe. A 2011 review of worldwide privacy laws revealed that twenty-five of the twenty-nine non-European countries with data privacy laws had "border control data export limitations," although the review noted the strength of those limitations "varies a great deal, and [the limitations] are not yet in force in the laws of Malaysia and Hong Kong."[27] As one scholar noted, it is no surprise that the adequacy approach has been adopted in many countries because the Directive has had a significant worldwide impact in encouraging "the rise of omnibus legislation throughout the EU and most of the world" modeled on the Directive (including its adequacy mechanism).[28]

Both the United States and Europe are considering major overhauls to their respective privacy regimes. In January 2012, the European Commission unveiled a proposed regulation[29] to supplant the existing Directive (the "Proposed Regulation"). Unlike a directive, which requires each EU Member State to pass implementing legislation, an EU regulation is directly binding on all Member States.[30] Thus, the proposal seeks to further harmonize EU data privacy law by establishing uniform data protection requirements across all EU Member States. In addition, the Proposed Regulation might also add new privacy rights, such as the so called

---

26. APEC, PRIVACY FRAMEWORK 28 (2005), *available at* http://publications.apec.org/publication-detail.php?pub_id=390.

27. Graham Greenleaf, *Do Not Dismiss 'Adequacy': European Data Privacy Standards Are Entrenched*, 114 PRIVACY L. & BUS. REP. 16–17 (Dec. 2011) [hereinafter Greenleaf, *Do Not Dismiss*].

28. Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. (forthcoming 2013); *see also id.* (attributing the spread to "harmonization networks," because worldwide privacy policymaking "has not been led exclusively by the EU, but has been a collaborative effort marked by accommodation and compromises").

29. *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, COM (2012) 11 final (Jan. 25, 2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf [hereinafter *Proposed Regulation*].

30. *See* EUROPEAN UNION, REGULATIONS, DIRECTIVES & OTHER ACTS (last visited Sept. 4, 2013), http://europa.eu/eu-law/decision-making/legal-acts/index_en.htm.

"right to be forgotten," by which individuals could request information about themselves be removed from the Internet entirely.[31]

In February 2012, President Obama unveiled his Consumer Privacy Bill of Rights as part of his administration's comprehensive blueprint to enhance U.S. privacy protections.[32] The Privacy Bill of Rights calls for baseline privacy legislation largely modeled on the FIPPs.[33] Commissioner Brill remarked in her 2013 Brussels speech that the Bill of Rights reflects that "there is always room for improvement," which is why she supports such comprehensive privacy legislation even while recognizing the strength of the existing U.S. framework.[34] Separately, several agencies have recently updated the regulations associated with the privacy laws they enforce. For example, in December 2012, the Federal Trade Commission (FTC) updated the regulations protecting children's privacy.[35] And in January 2013, the Department of Health and Human Services (HHS) released a substantial update to health privacy regulations.[36]

Along with attempting to reshape their individual privacy frameworks, the United States and EU are working to establish a new trade agreement. In his 2013 State of the Union, President Obama announced the United States and EU would begin talks on a comprehensive Transatlantic Trade and Investment Partnership (TTIP).[37] A first round of TTIP negotiations took place in Washington D.C. on July 8–12. The second round of TTIP negotiations were set to take place in Brussels, Belgium, in October

31. *Id.* at art. 17; *see also infra* note 107 and accompanying text.

32. THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECT. PRIVACY & PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECON. (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

33. *Id.* at 47 (The Consumer Bill of Rights).

34. Brill, *supra* note 10, at 6.

35. *See* Children's Online Privacy Protection Rule, 78 Fed. Reg. 3972 (Jan. 17, 2013) (to be codified at 16 C.F.R. part 312).

36. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule, 78 Fed. Reg. 5566 (Jan. 25, 2013) (to be codified at 45 C.F.R. parts 160 and 164).

37. President Barack Obama, State of the Union Address (Feb. 12, 2013), *available at* http://www.c-span.org/uploadedFiles/Content/Documents/State-of-the-Union-2013.pdf.

2013.[38] Because modern trade invariably involves the transfer of personal data, the level of U.S. privacy protections and U.S. adequacy as determined by EU law likely will be a focus of the negotiations, as the parties attempt to develop a durable trade discipline facilitating the free flow of data while protecting privacy.[39]

Against this backdrop of evolving frameworks and trade negotiations, now is the time for earnest discussion about how U.S. privacy law compares to EU standards. This discussion should take into account the inherent cultural, political, and constitutional differences between the two legal systems. The United States and EU have the opportunity to work towards interoperability and mutual respect by recognizing how both of their approaches to privacy satisfy the core privacy protections embodied in international standards.

I. HOW THE ADEQUACY MECHANISM WORKS

The EU Data Protection Directive generally prohibits transfers of personal data to a third country unless that third country "ensures an adequate level of protection."[40] Article 26(1) lists six exceptions to the general requirement that a third country ensure an adequate level of protection.[41] Article 26(2) allows EU Member States to authorize

38. *In Focus: Transatlantic Trade and Inv. P'ship (TTIP)*, EURO. COMM'N, http://ec.europa.eu/trade/policy/in-focus/ttip/ (last visited Sept. 4, 2013).

39. *See, e.g.*, *EU Officials Want U.S. to Bolster Data Privacy Protections in Trade Talks*, INSIDE U.S. TRADE (Feb. 21, 2013), http://insidetrade.com/Inside-US-Trade/Inside-U.S.-Trade-02/22/2013/eu-officials-want-us-to-bolster-data-privacy-protections-in-trade-talks/menu-id-172.html; Christopher Wolf, *Trade Law and Privacy Law Come Together*, IAPP PRIVACY PERSP. (Feb. 21, 2013), http://www.privacyassociation.org/privacy_perspectives/post/trade_law_and_privacy_law_come_together.

40. Council Directive 95/46, *supra* note 19, art. 25(1) ("The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.").

41. Article 26(1) includes the following six exceptions:

a. the data subject has given his consent unambiguously to the proposed transfer; or

b. the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

transfers where "appropriate contractual clauses" are in place to provide "appropriate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights."[42]

The Directive, under Article 29, establishes a "Working Party on the Protection of Individuals with regard to the Processing of Personal Data" (the "Article 29 Working Party" or the "Working Party").[43] The Article 29 Working Party is responsible for, among other things, giving the European Commission its opinion on the level of protection in third countries.[44] Additionally, the European Commission may issue a decision that a third country ensures an adequate level of protection, which is binding on all EU Member States.[45]

The Directive provides very broad guidance on how to assess whether a third country ensures an adequate level of protection:

> The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question, and the

---

c. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
d. the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence [sic] of legal claims; or
e. the transfer is necessary in order to protect the vital interests of the data subject; or
f. the transfer is made from a register which according to laws or regulations is intended.

Council Directive 95/46, *supra* note 19, art. 26(1).

42. *Id.* art. 26(2).
43. *Id.* art. 29, 30.
44. *Id.* art. 30(1)(b).
45. *Id.* art. 25(6).

> professional rules and security measures which are complied with in that country.[46]

The Article 29 Working Party has issued two documents further discussing how adequacy of third countries should be assessed.[47] The Working Party states that Article 25 reflects a "case by case approach whereby the assessment of adequacy is in relation to individual transfers or individual categories of transfers."[48] Thus, the Working Party takes the position that even where a third country is generally deemed adequate, any given data transfer could still be prohibited.[49] Furthermore, there is nothing to stop the European Commission or an EU Member State from revoking an adequacy determination at any time.

The Article 29 Working Party has provided additional guidance for making adequacy determinations. The Working Party's broad conclusion is that "any meaningful analysis of adequate protection must comprise the two basic elements: the content of the rules applicable and the means for ensuring their effective application."[50] The Working Party identified six core data protection content principles[51] and three core procedural/enforcement requirements,[52] "compliance with which could be seen as a minimum requirement for

---

46. *Id.* art. 25(2).

47. *See* ARTICLE 29 WORKING PARTY, WP 4, FIRST ORIENTATIONS ON TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES—POSSIBLE WAYS FORWARD IN ASSESSING ADEQUACY (1997) [hereinafter WP 4]; ARTICLE 29 WORKING PARTY, WP 12, WORKING DOCUMENT: TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES: APPLYING ARTICLES 25 & 26 OF THE EU DATA PROTECTION DIRECTIVE (1998) [hereinafter WP 12].

48. WP 12, *supra* note 47, at 26.

49. *See id.* (noting that determinations that a third country generally ensures an adequate level of protection "would be 'for guidance only,' and therefore without prejudice to cases which might present particular difficulties").

50. *Id.* at 5.

51. The content principles are (1) the purpose limitation principle, (2) the data quality and proportionality principle, (3) the transparency principle, (4) the security principle, (5) the rights of access, rectification, and opposition, and (6) restrictions on onward transfers. *Id.* at 6. The 1998 Working Document also lists three additional principles for certain types of processing: sensitive data, direct marketing, and automated individual decision. *Id.* at 6–7.

52. The procedural/enforcement principles are (1) to deliver a good level of compliance with the rules, (2) to provide support and help to individual data subjects in the exercise of their rights, and (3) to provide appropriate redress to the injured party where rules are not complied with. *Id.* at 7.

protection to be considered adequate."[53] No other guidance has been issued since 1998, so any further observations about what constitutes an adequate level of protection must be adduced from the small number of adequacy determinations issued by the Article 29 Working Party and European Commission.[54]

As of this Article's writing, the European Commission has issued thirteen favorable adequacy determinations.[55] The Commission has recognized Andorra, Argentina, Australia, Canada, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, and Uruguay as ensuring adequate protection for all personal data transfers from the EU to those countries.[56] Additionally, the Commission has recognized adequate protection for some types of transfers to Canada[57] and the United States.[58]

It is worth noting, however, that nineteen European countries that are not part of the EU appear to enjoy a de facto adequacy determination. These countries have acceded to both Convention 108[59] and the Additional Protocol,[60] which together require signatories to have laws that meet all the key requirements of the EU Directive.[61] Thus, as one scholar notes, "no such country has bothered to apply for a[n] adequacy finding, even though they are the

53. *Id.* at 5.

54. *See, e.g.*, *supra* note 47.

55. *See Comm'n Decisions on the Adequacy of the Prot. of Personal Data in Third Countries*, EURO. COMM'N, http://ec.europa.eu/justice/data-protection/ document/international-transfers/adequacy/index_en.htm (last updated Jul. 16, 2013). Separately, the European Union has entered into agreements with Australia and the United States to allow the transfer of Passenger Name Record data by air carriers.

56. *Id.*

57. The Commission has recognized as adequate Canada's handling of Passenger Name Record (PNR) data and transfers to recipients subject to the Personal Information Protection and Electronic Documents Act (PIPEDA). *See* Commission Decision 2006/253, 2006 O.J. (L 91) 49 (PNR); Commission Decision 2002/2, 2002 O.J. (L 2) 13 (PIPEDA).

58. The Commission has recognized that the Safe Harbor Framework ensures an adequate level of protection. *See infra* note 131 and accompanying text.

59. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Eur. T.S. No. 108 (Jan. 28, 1981) [hereinafter Convention 108].

60. *Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows*, Eur. T.S. No. 181 (Nov. 8, 2001) [hereinafter *Additional Protocol*].

61. *See, e.g.*, Convention 108, *supra* note 59, ch. II (laying out privacy safeguards and data subject rights akin to EU Directive); *Additional Protocol*, *supra* note 60, art. 1 (requiring DPA); *id.* art. 2 (requiring adequacy determinations for nonparties to Convention 108).

most likely countries to be successful," because "there is, in practice, simply no need for an adequacy declaration."[62] And "the EU has in most cases awaited requests from third countries to initiate the process" of adequacy determinations.[63]

Other factors have further contributed to the low number of published adequacy determinations. Several commentators have noted that the EU could be "more pro-active and more transparent about its processes."[64] For example, the EU does not generally publish negative or unfavorable adequacy determinations.[65] The Article 29 Working Party has never made a negative adequacy opinion public, and the only published negative opinions come from external consultants.[66] The pool of adequacy opinions providing guidance therefore is quite limited.

A review of some of the published adequacy determinations reveals some trends and potential inconsistencies in how the adequacy mechanism has been employed in practice. For example, New Zealand is the most recent country to be deemed to ensure an adequate level of protection.[67] Professor Greenleaf notes, however, that the Article 29 Working Party opinion on New Zealand's adequacy "found seven instances of where New Zealand's content principles were not fully 'adequate.'"[68] Most noteworthy among these is that the Article 29 Working Party had concerns with New Zealand's restrictions on onward transfers to other countries (i.e., New Zealand's adequacy mechanism) and concluded that New Zealand law did not comply fully with the EU Directive on this point.[69] Yet the Article 29 Working Party seemed to downplay this concern due to New Zealand's "geographical isolation," "the size and

62. *See* Greenleaf, *Do Not Dismiss*, *supra* note 27, at 17.

63. Alex Boniface Mukalilo, *Data Protection Regimes in Africa: Too Far from the European 'Adequacy' Standard?*, INT'L DATA PRIVACY L., Nov. 2012, at 8.

64. Greenleaf, *Not Entirely Adequate*, *infra* note 68, at 17.

65. *Id.*

66. Mukalilo, *supra* note 63, at 8.

67. Commission Decision 2013/65, 2013 O.J. (L 28) 12.

68. Graham Greenleaf, *Not Entirely Adequate But Far Away: Lessons from How Europe Sees New Zealand Data Protection*, PRIVACY L. BUS. REP. 8 (July 2011) [hereinafter Greenleaf, *Not Entirely Adequate*].

69. ARTICLE 29 WORKING PARTY, WP 182, OP. 11/2011 ON THE LEVEL OF PROTECTION OF PERSONAL DATA IN NEW ZEALAND 9–10 (2011).

the nature of its economy," and the low probability that "significant volumes of EU-sourced data" would be transferred to third countries.[70]

In effect, the Article 29 Working Party's opinion on New Zealand's adequacy might highlight a tale of two standards. The decision reflects an underlying rationale that "[i]t will be relatively rare that personal data on EU citizens ends up in New Zealand, so a good deal of tolerance of variation from the core principles previously set out by the Working Party is permitted by them in delivering an adequacy opinion."[71] Meanwhile, "[i]n a country like India, where outsourcing of the processing of European data is of large scale, as are other forms of business and travel involving personal data, different considerations are likely to apply."[72] Professor Greenleaf concludes that the Article 29 Working Party's opinion reflects "significant pragmatic preparedness on the part of the Working Party."[73] But the opinion might also illustrate a different standard for large- versus small-scale data processing countries when seeking adequacy determinations.

Argentina's favorable adequacy determination illustrates other nuances in the EU's approach to adequacy. Argentina passed its comprehensive privacy law in October 2000, issued an implementing/clarifying regulation in December 2001, and then requested an adequacy determination from the EU in January 2002.[74] In October 2002, the Article 29 Working Party released its favorable adequacy opinion,[75] and in June 2003, the European Commission decided Argentina ensured an adequate level of protection.[76]

The Article 29 Working Party gave a favorable opinion on Argentina's adequacy despite substantial concerns with its procedural

70. *Id.* at 10 ("In reality, given the geographical isolation of New Zealand from Europe, its size and the nature of its economy, it is unlikely that New Zealand agencies will have any business interest in sending significant volumes of EU-sourced data to third countries.").

71. Greenleaf, *Not Entirely Adequate*, *supra* note 68, at 9.

72. *Id.* at 3.

73. *Id.* at 2.

74. ARTICLE 29 WORKING PARTY, WP 63, OP. 4/2002 ON THE LEVEL OF PROTECTION OF PERSONAL DATA IN ARGENTINA 2–3 (2002).

75. *Id.*

76. Commission Decision 2003/490, 2003 O.J. (L 168) 19.

and enforcement mechanisms.[77] For instance, the Working Party expressed concern that the Data Protection Authority (DPA) was not guaranteed to be independent and lacked jurisdiction over all data controllers and processors.[78] Moreover, the Working Party noted that it relied heavily on the Argentinean government's assurances with respect to how the law was being implemented.[79] Thus, the Working Party concluded by stressing that its opinion was "drafted on the basis of these assumptions and explanations and in the absence of any substantial experience with the practical application of the legislation."[80]

This conclusion stands in stark contrast to more recent adequacy opinions commissioned by the European Commission. For example, Burkina Faso was among four African countries that recently sought adequacy determinations from the EU.[81] The advisory opinion on Burkina Faso's adequacy "refrained from giving its conclusion whether Burkina Faso provides an 'adequate level of protection of personal data.'"[82] It based this decision in part on the opinion that "the existence of actual enforcement mechanisms is an important part of the criteria to meet before being possibly considered as a country offering an adequate protection in the sense of article 25."[83] Yet the Article 29 Working Party offered a favorable opinion for Argentina at a time when Argentina's DPA had issued no significant guidance and pursued no enforcement. Indeed, Argentina's low number of enforcement actions to date, coupled with insight gleaned from discussions with Argentinian practitioners, suggest that Argentina may still lack effective enforcement mechanisms in practice—even if effective mechanisms exist on paper.

Another issue with the adequacy mechanism is the potential for the process to become politicized. The Article 29 Working Party itself recognized the potential for political tensions surrounding adequacy determinations, noting that "some third countries might

77. *See* ARTICLE 29 WORKING PARTY, *supra* note 69, at 17.
78. ARTICLE 29 WORKING PARTY, *supra* note 69, at 14.
79. *Id.* at 17.
80. *Id.*
81. Mukalilo, *supra* note 63, at 1–2.
82. *Id.* at 4.
83. *Id.* at 5 (quoting advisory opinion).

come to see the absence of a finding that they provided adequate protection as politically provocative or at least discriminatory, in that the absence of a finding is as likely to be the result of their case not having been examined as of a judgment on their data protection system."[84] According to Mukalilo, this is why the EU generally avoids releasing negative adequacy opinions.[85] More troubling, although ultimately of no effect, was Ireland's objection in 2010 to the adequacy determination for Israel. After Israel received a favorable adequacy opinion from the Article 29 Working Party, Ireland officially objected and delayed the European Commission's decision.[86] Ireland raised its objection ostensibly based on minor concerns with the Israeli protections for manual data processing and the DPA's independence.[87] But Ireland admitted to making an objection for reasons wholly unrelated to privacy, as it was outraged by the use of fake Irish passports by alleged Israeli agents in a targeted killing.[88] Use of the adequacy mechanism to achieve unrelated political ends could threaten the legitimacy of the system and undermine third countries' confidence that their privacy regimes are being evaluated purely on the merits.

We are in the early days of modern international data privacy law—privacy law that addresses the use of technology—and it is understandable why the form of a nation's privacy law regime has been used as a convenient surrogate for adequacy. However, now that multiple national regimes have had the chance to mature, and regulators in Europe have had a decade or more to observe them, it's reasonable and desirable for the Article 29 Working Party to apply the full-factors approach that EU law allows them to use in recommending adequacy.[89]

---

84. WP 12, *supra* note 47, at 27.

85. Mukalilo, *supra* note 63, at 8.

86. Laurence Peter, *Ireland Delays EU Deal with Israel on Data Transfers*, BBC NEWS (Sept. 3, 2010), http://www.bbc.co.uk/news/world-europe-11176926.

87. *Id.*

88. *Id.*

89. The European Commission itself has had very few opportunities directly to consider adequacy and to bring the full range of stakeholder interests to bear in consideration of adequacy.

II. THE CASE FOR U.S. ADEQUACY

It has been said that the United States and England are two countries separated by a common language. Something similar can be said with respect to the United States and EU when it comes to privacy: both the United States and Europe fundamentally agree on the need for privacy protections and the core tenets of what those protections look like.[90] The differences are largely in form, not substance.

Privacy law worldwide has evolved from a set of core principles. As discussed earlier, the 1980 OECD privacy guidelines identified eight FIPPs to guide all data collection, use, and disclosure.[91] The OECD guidelines were formally ratified by twenty-four OECD member countries, including the United States and many European nations.[92] These eight FIPPs have been highly influential in the development of privacy laws and regulations worldwide.[93] The FIPPs form the foundation of almost every nation's information privacy protections, including both the U.S. and the European Union privacy regimes.[94] Historically, however, the EU and the United States have taken divergent approaches to implementing the FIPPs.

In the United States, the legal framework for information privacy has focused on providing protections tailored to specific areas of concern, such as health records and children's personal information.[95] This sectoral approach, with its focus on sensitive personal information, has deep roots in American law. In large part, it reflects

90. THE WHITE HOUSE, *supra* note 32, at 49 (Appendix B: *Comparison of the Consumer Privacy Bill of Rights to Other Statements of the Fair Information Practice Principles*).

91. *See* OECD, *supra* note 12, paras. 7–14 (identifying the eight FIPPs as collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability).

92. *See* OECD, LIST OF OECD MEMBER COUNTRIES—RATIFICATION OF THE CONVENTION ON THE OECD, *available at* http://www.oecd.org/general/listofoecdmember countries-ratificationoftheconventionontheoecd.htm (last visited Sept. 4, 2013).

93. DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 2013 208–10 (2013).

94. *See, e.g.*, John W. Kropf, *Independence Day: How to Move the Global Privacy Dialogue Forward*, BLOOMBERG BNA PRIVACY & SEC. L. REP., Jan. 2009, at 62 ("The Guidelines have been highly influential, and are at the heart of most countries' privacy legislation . . . .").

95. *See supra* notes 14, 16 and accompanying text.

that privacy interests are balanced with competing interests, such as the right to free speech and respect for free-market solutions.

The United States passed one of the very first privacy laws back in 1970, ten years before the OECD privacy guidelines, when Congress enacted the Fair Credit Reporting Act (FCRA).[96] At the time, there was widespread concern over how credit reporting agencies would use the vast troves of information becoming available through automated processing of credit transactions.[97] (Remember that computing was still in its infancy, and thus the ability to computerize record-keeping was just starting to revolutionize society.) As a result, Congress passed the FCRA to ensure the accuracy, fairness, and privacy of personal information assembled by the credit reporting agencies.

The next major U.S. privacy law came as a result of the Nixon administration's privacy abuses. Mere months after Nixon's resignation, Congress enacted the Privacy Act of 1974 to apply the FIPPs to U.S. federal agencies' collection, storage, use, and disclosure of the personal information of U.S. citizens.[98]

Starting in the 1980s, Congress enacted a series of privacy laws targeting specific sectors. These laws often passed in response to publicized incidents demonstrating a lack of privacy protections in a certain sector. For example, Congress enacted the Electronic Communications Privacy Act of 1986[99] in response to concerns with electronic surveillance technologies. Then, in 1988, Congress enacted the Video Privacy Protection Act[100] after a reporter published the video rental records of Robert Bork, at the time a Supreme Court nominee.[101]

The 1990s saw the passage of several blockbuster privacy laws in the United States. Congress enacted laws addressing health privacy,

---

96. Fair Credit Reporting Act of 1970, Pub. L. No. 91-508, tit. VI, 84 Stat. 1114, 1128 (1970) (codified as amended at 15 U.S.C. §§ 1681–81x).

97. Lacey Fosburgh, *23 to Study Computer 'Threat,'* N.Y. TIMES, Mar. 12, 1970, at 38.

98. Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (1974) (codified as amended at 5 U.S.C. § 552a).

99. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2510–22).

100. Video Privacy Protection Act, Pub. L. No. 100-618, 102 Stat. 3195 (1988) (codified as amended at 18 U.S.C. § 2710).

101. Editorial, *Video Viewers' Privacy*, MIAMI HERALD, Oct. 26, 1987, at 10A.

financial privacy, and children's privacy.[102] In each area, Congress enacted legislation that also called for the appropriate federal agencies to enact accompanying regulations fleshing out the details of the law. For example, Congress passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA) with minimal detail regarding health privacy protections. But the law called on the HHS to enact a detailed Privacy Rule.[103] This hybrid law-and-regulation approach has allowed Congress to pass high-level privacy guidance for a specific sector, and to give the federal agency with sector-specific subject matter expertise the authority to elaborate the nuances and address the low-level implementation details.

Perhaps the most significant legislative action on privacy in the United States, however, has come through state data breach notification statutes. California passed the first such law[104] in the early 2000s, and now almost every state, commonwealth, and territory in the United States has a similar statute.[105] Generally speaking, these laws require entities to notify affected individuals and/or regulators whenever entities experience a data breach. A data breach can include losing a computer or flash drive containing personal information, having an employee steal personal information to commit identity theft, or experiencing an attack that results in hackers gaining access to company databases.

The effect of these laws cannot be overstated. According to the Privacy Rights Clearinghouse, since 2005, over 3,700 breaches involving over 600 million compromised records have been reported under these state laws.[106] Breach notification laws have resulted in greater transparency into entities' privacy and security practices, as well as raising consumer interest in privacy protections. There are

---

102. *See supra* notes 14–16.

103. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 263(iii).

104. *See* CAL. CIV. CODE § 1798.29 (2012).

105. *See* NAT'L CONFERENCE OF STATE LEGISLATURES, STATE SEC. BREACH NOTIFICATION LAWS, http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx (last visited May 1, 2013) ("Forty-six states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information.").

106. *See Chronology of Data Breaches*, PRIVACY RIGHTS CLEARINGHOUSE, http://www.privacyrights.org/data-breach (updated Sept. 22, 2013) (providing a list of disclosed breaches).

obvious costs associated with a data breach, such as the money spent investigating and reporting the incident, and the costs associated with providing affected individuals with credit monitoring services.[107] Companies suffering a data breach also pay a reputational penalty, as consumers are less likely to trust the company with their business in the future.[108] The result has been an incredible increase in attention paid to preventing data breaches, with a resulting increase in privacy protections across the board.

United States privacy protections, however, are not limited to specific laws and regulations. The FTC has played an increasingly active role in shaping what privacy protections are expected for all U.S. businesses. The FTC Act gives the FTC authority to regulate all "unfair or deceptive practices or acts in or affecting commerce."[109] Starting in the 2000s, the FTC began to invoke this authority to govern companies' privacy practices. Commissioner Brill has stated that "privacy protection is 'mission critical'" at the FTC.[110]

The FTC has acted through two mechanisms. First, the FTC has brought scores of enforcement actions concerning privacy.[111] The earliest actions focused on holding companies to the promises included in their online privacy policies; violation of a privacy promise constituted a deceptive practice under the FTC Act.[112] Increasingly, however, the FTC has invoked its authority to affirmatively state what privacy practices are reasonably expected for all companies. Recent FTC enforcement actions have resulted in

107. *See* PONEMON INST., 2011 COST OF DATA BREACH STUDY (2012), *available at* http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-us.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2012Mar_worldwide__CODB_US (noting that the average breach results in a cost of approximately $200 per compromised record).

108. VIRGINIA CITRANO, ADVISEN, THE REPUTATIONAL RISK OF DATA BREACH 11 (Sept. 2012), *available at* http://corner.advisen.com/pdf_files/Reputational_Risk_Data_Breach_2012NAS.pdf.

109. *See* 15 U.S.C. § 45 (2013).

110. Brill, *supra* note 10, at 2.

111. For a listing of the FTC's enforcement actions, *see* FTC BUREAU OF CONSUMER PROT., LEGAL RESOURCES, http://business.ftc.gov/legal-resources/all/35 (last visited May 1, 2013).

112. *See* FTC v. Twitter Inc., No. 092 3093.

settlements whereby the company agrees to implement a comprehensive and auditable privacy program.[113]

Second, and complementary to its enforcement efforts, the FTC has increasingly sought to provide companies guidance on privacy best practices. To that end, the FTC has published a series of reports, most recently on issues regarding privacy in mobile apps.[114] In March 2012, the FTC also published a fairly comprehensive guide to privacy best practices.[115] Moreover, the FTC has convened workshops to promote broad discussions regarding privacy issues.[116] These workshops bring together the regulators, company and industry representatives, and privacy advocates to debate the appropriate privacy safeguards that should be considered best practices. These workshops often result in publication of reports or guidelines summarizing the FTC's advice—which then become the baseline by which the FTC brings future enforcement actions.

The net impact of the FTC's two mechanisms has been to raise the privacy floor. Companies doing business in the United States are now expected to have published privacy policies and privacy programs—even though no federal law imposes these requirements on the vast majority of businesses (with the exception of companies operating in highly regulated sectors, such as healthcare). And the thousands of companies that have self-certified to the Safe Harbor Framework[117] (which allows personal data to be transferred from the EU to the U.S., as discussed below)[118] have both imposed these

113. Shayndi Raice & Julian Angwin, *Facebook 'Unfair' on Privacy*, WALL ST. J., Nov. 30, 2011, *available at* http://online.wsj.com/article/SB10001424052970203441704577068400622644374.html ("As part of the settlement, Facebook agreed to submit to independent privacy audits every two years for the next 20 years.").

114. *See* FTC, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY (Feb. 2013), *available at* http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf.

115. *See* FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUS. & POLICYMAKERS (2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

116. *See, e.g.*, *The Big Picture: Comprehensive Online Data Collection*, FTC (Dec. 6, 2012), *available at* http://ftc.gov/bcp/workshops/bigpicture/.

117. *See, e.g.*, EU-U.S. Joint Statement, *supra* note 2 (noting "over 3,000 companies have self-certified" to the Safe Harbor Framework).

118. *See infra* notes 128–130 and accompanying text.

requirements on themselves and subjected themselves to FTC enforcement.

There are also significant extra-legal forces operating in the United States that contribute to providing broad privacy protections. For example, the past fifteen years has seen an explosion in companies hiring Chief Privacy Officers (CPOs). In 2000, the few companies that had created CPO positions actually issued press releases announcing their actions.[119] Now there are thousands of CPO positions at companies across the United States. The existence of a C-level position focused on privacy elevated corporate America's focus on privacy and resulted in substantial increases in time and resources devoted to privacy protections.

The privacy profession has been further enhanced through professional associations. A professional organization known as the International Association of Privacy Professionals (IAPP) was formed in 2000 to provide a venue for CPOs to discuss privacy issues and share best practices.[120] In early years, the IAPP had conferences where numerous CPOs would gather to share knowledge. For the 2013 Global Privacy Summit,[121] over 2,000 people were in attendance. The organization now boasts more than 10,000 members in the United States alone, and provides numerous certifications for individuals seeking to establish their credentials as privacy professionals in the marketplace.

There are also numerous privacy lawyers—working with policymakers, engineers, and others—engaged in privacy compliance advice, representation, advocacy, and scholarship. Privacy law articles have influenced privacy professionals and policymakers alike. The field of privacy law itself originated with the seminal law review article by Warren and Brandeis on *The Right to Privacy*.[122] Additionally, privacy advocacy groups have increased

119. *See, e.g.*, Press Release, IBM, IBM Names Harriet P. Pearson as Chief Privacy Officer (Nov. 29, 2000), *available at* http://www-03.ibm.com/press/us/en/pressrelease/1464.wss.

120. *See About the IAPP*, INT'L ASS'N PRIVACY PROF'L, https://www.privacyassociation.org/about_iapp (last visited Sept. 4, 2013).

121. *See Global Privacy Summit 2013*, INT'L ASS'N PRIVACY PROF'L, https://www.privacyassociation.org/events_and_programs/global_privacy_summit_2013 (last visited May 1, 2013).

122. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV.

their watchdog role to play a significant role in prompting enforcement. Many FTC enforcement actions start with complaints filed by these very advocacy groups.[123]

Finally, litigation has served as a backstop to keep pressure on companies to implement and maintain robust privacy programs. These days, a company announcement of a data breach or media reports on a privacy slip-up frequently result in the filing of class action lawsuits within days of the news. While these class action suits on the whole have not been generally successful in establishing liability and damages,[124] they have provoked numerous settlements from companies averse to public litigation with customers. The cases increase the bottom line costs that companies weigh in deciding how they allocate their resources, and that weighing means increased attention to privacy programs.

Berkeley professors Ken Bamberger and Deirdre Mulligan have extensively researched the role that extra-legal forces play in protecting privacy. In their landmark study of privacy "on the ground," they interviewed several CPOs to assess the state of privacy protections in the United States.[125] Their findings suggest that the extra-legal forces described above, coupled with the various laws and regulations on the books, have resulted in privacy becoming more embedded into U.S. corporate culture and business operations.[126] More importantly, their research suggests that

193 (1890).

123. *See, e.g.*, *Facebook Privacy*, EPIC.ORG, http://epic.org/privacy/facebook/ (last visited Sept. 18, 2013) ("The settlement follows from complaints filed by EPIC and other consumer and privacy organizations in 2009 and 2010 over Facebook's decision to change its users' privacy settings in a way that made users' personal information more widely available to the public and to Facebook's business partners."); Byron Acohido, *Group Urges FTC Action on Google Privacy*, USA TODAY, Feb. 8, 2012, *available at* http://usatoday30.usatoday.com/tech/news/story/2012-02-08/google-privacy-ftc/53014496/1 ("A lengthy FTC deceptive practices probe of Buzz, sparked by an EPIC complaint, resulted in Google agreeing to a consent order that prohibits the company from misrepresenting its privacy practices.").

124. *But see* Des Hogan, Michelle Kisloff, Christopher Wolf & James Denvil, *Regulators and Plaintiffs' Lawyers Are Ready to Pounce on Privacy and Data Security Missteps: A Guide to Limiting Corporate Risk*, BLOOMBERG BNA PRIVACY & SEC. L. REP., 12 PVLR 586 (Apr. 8, 2013), *available at* http://www.hldataprotection.com/files/2013/04/PDFArtic.pdf (noting that "[t]he plaintiffs' bar has won a string of recent victories in privacy class actions, which could light a path for others seeking to bring similar cases").

125. *See* Bamberger & Mulligan, *supra* note 18.

126. *See id.* at 314.

formalistic reviews of privacy "on the books" might substantially underestimate the strength of a third country's privacy protections overall.

III. SO WHY ISN'T THE UNITED STATES CONSIDERED ADEQUATE?

Despite the various layers contributing to robust privacy protections in the United States, the EU continues to view the U.S. privacy framework as inadequate under EU law—although the issue has never been squarely addressed, as the United States has never applied for a finding of adequacy, and the EU has never stated that it has denied or would deny any U.S. application. When the Directive entered into force in 1998, however, it was widely accepted that the United States lacked adequate privacy protections to qualify as adequate under EU law.[127] Thus, the United States and EU promptly began negotiating a way for U.S. businesses to be able to engage in certain international data transfers involving EU personal data. The U.S. goal was to create a "safe harbor" under which some U.S. businesses could receive EU personal data.[128] The challenge, however, was to bridge the gap between two very different approaches to privacy protections.

It took two years of negotiating, but eventually both sides reached an agreement that was acceptable to all. The result was the Safe Harbor Framework.[129] The Framework requires eligible companies to certify their compliance with seven broad principles: (1) notice, (2) choice, (3) restrictions on third-party transfers, (4) security for personal data, (5) data integrity, (6) individual access rights, and

127. *See, e.g.*, ARTICLE 29 WORKING PARTY, WP 15, OP. 1/99 CONCERNING THE LEVEL OF DATA PROTECTION IN THE UNITED STATES & THE ONGOING DISCUSSIONS BETWEEN THE EUROPEAN COMMISSION & THE UNITED STATES GOVERNMENT 2 (1999) ("[T]he Working Party takes the view that the current patchwork of narrowly-focused sectoral laws and voluntary self-regulation cannot at present be relied upon to provide adequate protection in all cases for personal data transferred from the European Union.").

128. *U.S.-EU Safe Harbor Overview*, EXPORT.GOV, http://export.gov/safeharbor/eu/eg_main_018476.asp (last visited Sept. 4, 2013) ("In order to bridge these differences and provide a streamlined and cost-effective means for U.S. organizations to satisfy the Directive's "adequacy" requirement, the U.S. Department of Commerce in consultation with the European Commission developed a "safe harbor" framework.").

129. The U.S. government maintains all documentation associated with the EU-U.S. Safe Harbor Framework online, *available at* http://export.gov/europeanunion/index.asp.

(7) submission to the FTC's jurisdiction for enforcement purposes.[130] In 2000, the European Commission recognized the Safe Harbor Framework ensured an adequate level of protection under the EU Directive,[131] and the Safe Harbor Framework has facilitated cross-border data transfers for thousands of companies in the intervening years.

Only companies subject to the jurisdiction of the FTC are eligible for participation in the Safe Harbor (as the FTC is the agency charged with enforcing Safe Harbor principles).[132] Thus, broad swaths of U.S. commerce, including transportation companies, communication common carriers, certain regulated financial services firms, and non-profits, are not eligible to participate in the Safe Harbor.

After the 9/11 attacks, the United States and EU entered into a separate arrangement providing for the sharing of airline passenger information involving EU personal data.[133] This second agreement allowed for the transfer of Passenger Name Records to U.S. government authorities for anti-terrorism purposes.[134]

These are the two primary agreements existing between the United States and EU regarding international data transfers.[135] As previously noted, the United States has never formally sought a full adequacy determination, but it is no secret the EU sees major shortcomings in the U.S. regime. The principal perceived shortcomings are that the EU generally disfavors a sector-by-sector approach, instead viewing comprehensive legislation as the superior method to ensure privacy protections.[136] Additionally, the EU

130. *See infra* note 132.

131. *See* Commission Decision 2000/520, 2000 O.J. (L 215) 7.

132. *Safe Harbor Enforcement*, EXPORT.GOV, http://export.gov/safeharbor/eu/eg_main_018481.asp (last updated Jan. 30, 2009).

133. *See* Commission Decision 2007/551, 2007 O.J. (L 298) 29.

134. *Id.* art. 1(1) ("For this purpose, this agreement sets forth the responsibilities of the Parties with respect to the conditions under which PNR may be transferred, processed and used, and protected.").

135. There have been other discussions and understandings reached regarding specific types of transactions, such as data transfers for anti-terrorism purposes, but these are beyond the scope of this Article.

136. *See, e.g.*, Peter Schaar, *Transatlantic Free Trade Zone? But Only When the U.S. Provide Improved Data Protection!*, GERMAN FED. COMM'R DATA PROT. FREEDOM INFO. BLOG (Feb. 13, 2013), http://www.bfdi.bund.de/EN/PublicRelations/SpeechesAndInterviews/blog/TransatlanticFreeTradeZone.html?nn=408870 ("Looking into data protection in the

considers the lack of an independent data protection authority in the United States to be a serious shortcoming.[137]

Some in the EU also criticize the effectiveness of the Safe Harbor.[138] These criticisms arise despite the European Commission's continuing support for the Safe Harbor Framework's adequacy, which was reaffirmed even after the release of the Proposed Regulation.[139] And evidence suggests the Safe Harbor Framework has played a key role "in raising privacy awareness and acceptance of privacy protection in the United States."[140]

The sectoral approach that has garnered European criticism has some advantages that might be underappreciated in Europe. For example, U.S. privacy law has been tailored across sectors to provide varying levels of protection appropriate for the sensitivity and use of personal information. This flexibility also permits quicker changes in response to new threats to privacy, without having to establish rigid protections that prevent flexibility. As to health privacy in the United States, for example, a detailed and robust framework exists under HIPAA.

U.S. the diagnosis is not assuring. Generally applicable rules for data protection in the private sector still are lacking. Measures taken in this area present the outlook of a more or less incomplete patchwork situation. The data protection rules in the 50 U.S. states are mostly inconsistent and incomplete. Only in certain sectors, such as health care, we can find data protection rules at all.").

137. *EU Comm'r criticises U.S. for the data prot. negotiations*, EURO. DIGITAL RIGHTS, http://www.edri.org/book/export/html/2493 ("Reding wants to obtain limitations of retained data, a strict ban on the transfer of data to other countries and asks for an independent data protection supervisor to be appointed by the U.S. for the supervision of the authorities' use of citizen data, as there is in Europe.").

138. *Id.*

139. *See* EU-U.S. Joint Statement, *supra* note 2 ("[T]he United States and the European Union reaffirm their respective commitments to the U.S.-EU Safe Harbor Framework. This Framework, which has been in place since 2000, is a useful starting point for further interoperability."). Note, however, that the official Rapporteur for the proposed Regulation proposed there be a regular reevaluation of the Safe Harbor arrangement. *See* JAN PHILIPP ALBRECHT, EUROPEAN PARLIAMENT, DRAFT REPORT ON THE PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT & OF THE COUNCIL ON THE PROT. OF INDIVIDUAL WITH REGARD TO THE PROCESSING OF PERSONAL DATA & ON THE FREE MOVEMENT OF SUCH DATA (GENERAL DATA PROT. REGULATION) 144–47 (2013), *available at* http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf.

140. Damon Greer, *Safe Harbor—A Framework that Works*, 1 INT'L DATA PRIVACY L. 143, 147 (2011).

The EU believes the United States affords too much governmental access to personal data, and that also affects its view of the U.S. privacy framework.[141] These concerns are rooted in the powers authorized by the U.S. Patriot Act, which was passed after the 9/11 attacks.[142] It is true the Patriot Act provides the U.S. government with authority to access personal data in certain situations.[143] But the EU is wrong to paint the U.S. government's access as exceptional. A legal review of ten different countries across the globe assessed their governments' level of access to information stored in the cloud.[144] The survey included the United States, several European countries, Canada, Australia, and Japan.[145] The results were clear: all ten countries permitted their governments similar levels of access to data stored in the cloud in the interests of national security and law enforcement.[146] And several countries actually enabled entities voluntarily to share such information with the government, without legal protections; the United States was not one of them.[147]

Finally, the EU criticism of the lack of a centralized enforcement authority for privacy in the United States should not be dispositive. The FTC has broad but not unlimited jurisdiction to police privacy violations in the United States. Influential scholars have made the case that enforcement efforts in the United States are very strong.[148]

---

141. Letter from Jacob Konstamm, Chairman, Article 29 Working Party, to Viviane Reding, Commissioner, Directorate-General for Justice, Fundamental Rights and Citizenship (Aug. 13, 2013), *available at* http://www.hldataprotection.com/files/2013/08/20130813_letter_to_vp_reding_final_en1.pdf.

142. 50 USC § 1861—Access to certain business records for foreign intelligence and international terrorism investigations (2001).

143. *Id.* (a)1.

144. *See* Winston Maxwell & Christopher Wolf, *Hogan Lovells White Paper on A Global Reality: Governmental Access to Data in the Cloud* (2012), *available at* http://m.hoganlovells.com/files/News/c6edc1e2-d57b-402e-9cab-a7be4e004c59/Presentation/NewsAttachment/a17af284-7d04-4008-b557-5888433b292d/Revised%20Government%20Access%20to%20Cloud%20Data%20Paper%20(18%20July%2012).pdf.

145. *Id.* at 6–12.

146. *Id.*

147. *See id.* at 13 (presenting a chart showing countries that allowed voluntary disclosure of personal data in response to informal governmental requests).

148. *See, e.g.*, Bamberger & Mulligan, *supra* note 18; Brill, *supra* note 10, at 6.

This is especially so when one considers the robust and increasing enforcement activity at the state level.[149]

Complicating matters, however, is the potential for greater separation between the U.S. and EU privacy regimes once the EU adopts the Proposed Regulation. The Proposed Regulation includes several elements not reflected in current or proposed U.S. law. For example, the Proposed Regulation would give individuals a "right to be forgotten," which would allow individuals to compel deletion of their personal data.[150] In the United States, such a right would likely run afoul of the First Amendment. Additionally, the Proposed Regulation would provide a "right to data portability."[151] Finally, the Proposed Regulation would expand the privacy rules' jurisdictional reach directly to companies processing EU personal data outside the EU.[152] U.S. privacy law, however, remains restricted to governing companies located within the United States, and instead makes the companies that transfer personal information outside the United States accountable for the actions of their third parties operating abroad.

The day after President Obama announced the new trade negotiations with the EU, the U.S. Trade Representative highlighted "the issue of cross-border data flows as one of those next-generational issues that should be addressed" during the negotiations.[153] That same day, an EU data protection official noted that the trade negotiations would present an opportune time to

149. *See, e.g.*, *Privacy in the Digital Age*, NAT'L ASS'N ATT'Y GEN., http://www.naag.org/privacy-in-the-digital-age.php (last visited May 1, 2013) (describing the 2013 nationwide focus by state attorneys general on addressing privacy issues).

150. *Proposed Regulation*, *supra* note 29, art. 17 (providing in enumerated circumstances that a "data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data").

151. *Proposed Regulation*, *supra* note 29, art. 18 (providing data subjects with the right to obtain a copy of their personal data and transfer it to another system).

152. *Proposed Regulation*, *supra* note 29, art. 3(2) ("This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to: (a) the offering of goods or services to such data subjects in the Union; or (b) the monitoring of their behaviour.").

153. Ron Kirk, U.S. Trade Representative, Transcript of Press Conference (Feb. 13, 2013), *available at* http://www.ustr.gov/about-us/press-office/pressreleases/2013/february/transcript-briefing-us-eu.

"broaden the insufficient level of data protection in the [United States]."[154]

The EU critique of the U.S. approach to privacy overlooks fundamental structural differences between the two legal regimes. For example, the United States has had to balance its robust privacy protections against strong constitutional protection for free expression. At times, the constitutional protections of the First Amendment may trump otherwise strong privacy interests.[155] In the EU, by contrast, the balance between the rights to privacy and free expression is less clear—but wherever the exact line falls, the protections for free expression in the EU do not rise to the level of First Amendment protections.[156]

While many EU Member States employ a civil law system, the United States has a rich history of relying on the common law. Indeed, the FTC's "enforcement efforts have established what some scholars call 'the common law of privacy' in the United States."[157]

CONCLUSION

Despite their similar origins in the FIPPs, the U.S. and EU privacy regimes have evolved in different ways over the past forty years. But their differences do not necessarily suggest a lack of equivalence or

154. Schaar, *supra* note 136.

155. *See, e.g.*, Florida Star v. B.L.F., 491 U.S. 524 (1989) (holding a Florida statute prohibiting the publication of names of victims of sexual offenses violated the First Amendment); Jacob Gershman, *When the First Amendment Trumps Privacy Concerns*, WALL ST. J. L. BLOG (Apr. 10, 2013), http://blogs.wsj.com/law/2013/04/10/when-the-first-amendment-trumps-privacy-concerns/ (noting that a magazine's publication of recordings from private meetings likely is protected by the First Amendment); *see also* Sorrell v. IMS Health Inc., 131 S. Ct. 2653 (2011) (holding a Vermont statute restricting the sale, disclosure, and use of prescription records violated the First Amendment).

156. *See, e.g.*, William Echikson, *Judging Freedom of Expression at Europe's Highest Court*, GOOGLE EURO. BLOG (Feb. 26, 2013), http://googlepolicyeurope.blogspot.com/2013/02/judging-freedom-of-expression-at.html (discussing litigation currently pending before the European Court of Justice involving Spanish citizens' efforts to have Google remove search results about them); Peter Fleischer, *The Saga Continues . . . Now to the Italian Supreme Court*, PRIVACY . . . ? (Apr. 17, 2013), http://peterfleischer.blogspot.com/2013/04/the-saga-continues-now-to-italian.html (discussing the continuing legal case involving Italy's prosecution of Google executives for violating Italian privacy law by not taking preemptive steps to block a user-uploaded video containing bullying from being posted).

157. Brill, *supra* note 10, at 3 (citing, *inter alia*, Bamberger & Mulligan, *supra* note 18).

interoperability to satisfy common goals. As Commissioner Brill notes, "[A]lthough the U.S. may for historic reasons approach privacy through our different legal tradition—one that uses a framework approach, backed up by strong enforcement—I believe this approach achieves many of the same goals as those embraced by EU data protection authorities."[158]

Why, then, has the U.S. approach been consistently viewed as providing an inadequate level of protection by EU officials? The reason seems to be the EU's emphasis on the form of a third country's privacy framework, rather than its substance. This trend is evidenced in the Article 29 Working Party's published adequacy opinions, as well as several statements by EU data protection officials, in emphasizing the differences in the U.S. approach.

As noted previously, however, there is substantial common ground between the two approaches, and many differences can be attributed to fundamental characteristics of the respective regimes. As Commissioner Brill observes, "We will not erase the differences in our privacy regimes. And . . . we need not erase them, because we have plenty of common ground for mutual recognition of our different, but equally effective, privacy frameworks."[159] In many other contexts, legal interoperability is achieved by recognizing these fundamental differences and embracing a flexible approach to managing cross-border issues.

Furthermore, the Article 29 Working Party's reliance to date on form as a surrogate for effectiveness of a nation's privacy regime overlooks the robust privacy protections currently available in the United States, as well as the different constitutional and legal structures in place. The Safe Harbor Framework has demonstrated one possible approach to mutual recognition and interoperability, and indeed the United States and EU have continued to reaffirm their commitment to that approach even as both sides consider revisions to their respective privacy frameworks.[160] The United States and EU

158. *Id.* at 6.

159. *Id.*

160. *See* EU-U.S. Joint Statement, *supra* note 2 ("In line with the objectives of increasing trade and regulatory cooperation outlined by our leaders at the U.S.-EU Summit, the United States and the European Union reaffirm their respective commitments to the U.S.-EU Safe Harbor Framework.").

jointly referred to the Safe Harbor Framework in March 2012 as "a useful starting point for further interoperability."[161]

The TTIP presents a golden opportunity to embrace interoperability outright and recognize solutions that give credit to the different ways the two systems achieve substantially similar aims. Perhaps foreshadowing the TTIP negotiations, the EU-U.S. joint statement in March 2012 included the following proclamation:

> As the EU and the United States continue to work on significant revisions to their respective privacy frameworks over the next several years, the two sides will endeavor to find mechanisms that will foster the free flow of data across the Atlantic. Both parties are committed to work towards solutions based on non-discrimination and mutual recognition when it comes to personal data protection issues which could serve as frameworks for global interoperability that can promote innovation, the free flow of goods and services, and privacy protection around the world.[162]

Part of that effort to find solutions rooted in mutual recognition should be a fresh look at the overall adequacy of the U.S. framework.

More flexible approaches to cross-border data transfers could provide robust privacy protections while facilitating free trade and the free flow of information. As Commissioner Brill noted, "Given the complexity of international data flows and different legal regimes around the globe, I think that providing more flexibility for cross-border data transfers could enhance privacy protection, spur innovation and trade, and help us achieve interoperability between our two systems."[163] Whether that flexibility arises within the framework of the EU adequacy approach, the TTIP trade agreement, or alternative measures, the end result should be the same: it is time for the United States and EU to reach a workable long-term solution to facilitating cross-border data transfers that both protects privacy and promotes international economic growth.

---

161. *Id.*
162. *Id.*
163. Brill, *supra* note 10, at 5–6.